Michigan Cyber Initiative News

April 2013, Issue 14

Articles of Interest

Pentagon Forming Cyber Teams to Prevent Attacks
The Defense Department is forming cyber teams to carry out operations to combat the threat of an electronic assault on the U.S. that could cause major damage and disruption to the country's vital infrastructure. — Read this article here.

Google Rolls Out Initiative to Help Hacked Sites
Google aims to answer questions about why a site was hacked, what malware may have been used, and how to wipe the site clean of bugs. — Read this article here.

Private Data Revealed by Facebook 'Likes': Study
Research shows patterns from these Facebook preferences can provide surprisingly accurate estimates of the user's race, age, IQ, sexuality and other personal information. — Read this article here.

Outdated Java Weak Spots are Widespread, Websense Says
Researchers say the latest version of Java is only in use by a dismal 5 percent of users, and many versions are months or years out of date — Read this article here.

Five Places Where You Should Never Give Your Social Security Number
Almost every day somebody asks for your Social Security Number and you probably give it up without giving it a second thought -- because that's what you've always done. — Read this article here.

Did You Know?

Is your organization prepared for a cyber attack?

There are many steps that should be taken to ensure you are prepared. If you have an established IT security team, you should consider asking these questions:

- How is our executive leadership informed about the current level and business impact of cyber risks to our company?
- What is the current level and business impact of cyber risks to our company? What is our plan to address identified risks?
- How does our cybersecurity program apply industry standards and best practices?
- How many and what types of cyber incidents do we detect in a normal week? What is the threshold for notifying our executive leadership?
- How comprehensive is our cyber incident response plan? How often is it tested? How are we continually making it better?

The source of these questions can be found here.

Advanced Persistent Threat

A global cybersecurity survey of more than 1,500 security professionals found that one in five respondents' enterprises experienced an advanced persistent threat (APT) attack.

ISACA further stated that 94 percent of APTs represent a credible threat to national security and economic stability and concluded that most enterprises are employing ineffective technologies to protect themselves.

The survey also revealed that the majority of respondents believe the use of social networking sites and personal devices, combined with rooting or jailbreaking the device, make a successful APT attack more likely.

Read this full article, more about APTs, and ISACA here.

Lawsuits Challenge Privacy Policies

Internet privacy has long been a hot-button issue. Central questions are being asked about who owns what data, how that data can be used by various companies to target individuals in marketing and whether users can opt-in or opt-out of various data-sharing approaches. Just as in other areas of life in America in 2012, these questions are often settled in the courts.

Now, Google is facing a class action lawsuit over its new privacy policy. Computerworld reported that Google faces complaints that they changed earlier privacy policies which promised that information obtained by one service will not be used by another service. Beyond consumer complaints and online criticism, a new group seeks to bring nationwide class action on behalf of holders of Google accounts and owners of Android devices from Aug. 19, 2004 to Feb. 29, 2012, who continued to maintain the Google accounts and own the devices after the new privacy policy came into effect on March 1 this year.

Here's an excerpt from the Computerworld article:

"The Internet company is being charged in both lawsuits for violation of the Federal Wiretap Act, for willful interception of communications and aggregation of personal information of its consumers for financial benefit, and the Stored Electronic Communications Act for exceeding its authorized access to consumer communications stored on its systems. Google is also charged with violation of the Computer Fraud Abuse Act, and other counts including state laws. …

The company's new privacy policy is already under scrutiny in the European Union and in the U.S., where 36 state attorneys general wrote to Google CEO Larry Page last month saying that Google's new policy does not give users a sufficient chance to opt out."

Other groups tried to block Google's privacy policy before it came into effect on March 1, but they were not successful in stopping the new policy from taking effect.

Google declined to comment on the lawsuits.

But Google is not alone. Last year Microsoft was sued over a phone-tracking feature. Here's a quote from the *Wall Street Journal* last September:

"A Michigan woman is suing Microsoft Corp. for alleged-tracking phones that run the software giant's Windows Phone 7 operating system, the centerpiece of the company's efforts to grab part of the burgeoning mobile market.

The suit, filed in the U.S. District Court in Seattle, alleges the operating system collects data about a user's whereabouts even after the software's tracking feature is ostensibly disabled. The suit, filed by Rebecca Cousineau, accuses Microsoft of violating various communications and privacy laws and seeks class-action status. …"

In reality, the list of lawsuits regarding privacy policy changes is fairly long, and I suspect that it will get longer over the next few years. Companies want to use your data in new ways, and this information about us is very valuable. These fears of data misuse can be either overblown or valid, depending on the situation. However, I am still a big believer that users should control how their information is shared and used. In addition, end users should be able to opt-in or opt-out of various tracking mechanisms. Of course, companies have the right to offer a discount or better service in return for the right to share information with partners or other company services.

One final point, with related headlines coming out from *Wired* magazine about NSA spying on our emails and plans for access to "deep data" or "deepnet" (which is password-protected information), I don't see these privacy issues being resolved anytime soon. Another article from the UK *Daily Mail* recently reported that the CIA wants to spy on us through our TVs (which I don't believe). Nevertheless, I think more privacy lawsuits are on the way. In my opinion, these topics will continue to be front and center for the next decade.

Author: Dan Lohrmann is the Chief Security Officer for the State of Michigan.